

REMARKS/ARGUMENTS

The Office Action of September 11, 2008 has been reviewed and carefully considered.

Reconsideration of the above-identified application, as herein amended, is respectfully requested.

Status of the Application

Claims 1-19, with claims 1 and 15 being independent, remain pending in this application, and new dependent claims 20 and 21 have been added. No new matter has been added.

In the Office Action of September 11, 2008, claims 16-19 were objected to; claims 1 and 2 were rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Patent No. 5,815,665 ("Teper") in view of U.S. Patent Publication No. 2002/0103999 ("Camnisch"); claims 3 and 4 were rejected under 35 U.S.C. §103(a) as unpatentable over Teper in view of Camnisch, and further in view of U.S. Patent Publication No. 2002/0085713 ("Feig"); claims 5, 6 and 8 were rejected under 35 U.S.C. §103(a) as unpatentable over Teper in view of Camnisch and Feig, and further in view of U.S. Patent No. 6,397,329 ("Aiello"); claim 7 was rejected under 35 U.S.C. §103(a) as unpatentable over Teper in view of Camnisch and Feig, and further in view of U.S. Patent Publication No. 2001/0011351 ("Sako"); claims 9 and 10 were rejected under 35 U.S.C. §103(a) as unpatentable over Teper in view of Camnisch and Feig, and further in view of U.S. Patent Publication No. 2001/0011351 ("Rupp"); claims 11-13 were rejected under 35 U.S.C. §103(a) as being unpatentable over Teper in view of Camnisch, and further in view of Sako; claim 14 was rejected under 35 U.S.C. §103(a) as unpatentable over Teper in view of Camnisch and Sako, and further in view of U.S. Patent No. 7,234,059 ("Beaver"); claim 15 was rejected

under 35 U.S.C. §103(a) as unpatentable over Feig; claim 16 was rejected under 35 U.S.C. §103(a) as unpatentable over Feig in view of Aiello; and claims 17 and 18 were rejected under 35 U.S.C. §103(a) as unpatentable over Feig in view of Sako. Applicants, after carefully considering the Examiner's rejections, together with the comments provided in support thereof, traverse these rejections and submit that the claims are patentably distinct over the applied references.

Information Disclosure Statement

The Examiner stated the documents that were cited in the Information statement (IDS) filed on September 5, 2008 fails to comply with the requirements of 37 CFR §1.98(a)(2). Applicants note, however, that the IDS that was not considered was filed on May 13, 2005. The Examiner did not consider the IDS because copies of the nonpatent literature publications were not supplied with the IDS. Applicants point out that the nonpatent literature publications listed on the SB/08 form were cited in the International Search Report and have accordingly already been supplied to the U.S.P.T.O. by WIPO; therefore, in accordance with U.S. practice, additional copies of those foreign references need not be submitted. For the Examiner's convenience, Applicants submit herewith a copy of the SB/08 form previously filed on May 13, 2005. Applicants request that the Examiner acknowledge and consider the references cited in the SB/08 form and return the acknowledged SB/08 form to Applicants.

Amendments

Claims 1-19 have been amended to improve the form thereof. New claims 20 and 21 have been added which further limit the respective claims from which they depend. Claims 1

and 15 have been amended to explicitly recite that a different or unique anonymous signature is used for each session. Support for this amendment can be found at least at page 12, line 10 and page 24, lines 19-26 of the specification as filed.

The Examiner has objected to claims 16-19 for reciting a method instead of a system. Claims 16-19 have been amended to recite a system. Withdrawal of the objection is requested.

The Present Disclosure

Disclosed is a method to provide secure access to data processing resources.¹ A general objective of the invention is to offer an anonymous user authentication service and a fast and economical mechanism for maintaining session authentication. Despite user anonymity, users are responsible for their actions because resources accessed during a session can revoke user anonymity if necessary, for example in the event of a dispute.

The method of accessing a service consists of identifying and registering a client, authenticating the client to an anonymous certification authority, authenticating the client by producing an anonymous signature, and opening and maintaining an anonymous authentication session with a server. For each session, the user provides a unique anonymous signature to the server. Selective contact is allowed between the server and the anonymous certification authority to revoke the anonymity of the client. The invention also relates to a system for opening and maintaining an authentication session guaranteeing non-repudiation, wherein for each session, the user provides a unique anonymous signature to the server.

¹ These descriptive details are provided only for the convenience of the Examiner as part of the discussion presented herein, and are not intended to argue limitations that are not claimed. Further, this is not intended to argue any interpretation of any claim term that is narrower than would be understood by one of ordinary skill in the art in the context of the specification and the claims as a whole.

In other words according to the disclosed method and a system configured to operate in accordance with the disclosed method, a user provides a server with a unique anonymous signature for each session. (Specification as filed, p. 24, ll. 19-26.). As described at page 11, lines 4-22 of the specification as filed, tokens corresponding to the claimed anonymous signature are calculated, which enable the user to open and maintain a session. Thus, if there are two different sessions started by the same user, each session -- whether or not they occur simultaneously -- cannot use the same anonymous signature and the fact that both sessions emanated from the same user cannot be determined so long as the anonymity is maintained.

Claims 1 and 15 and their dependent claims are patentable over the cited references

Among the recitations of amended independent claim 1 not present in the cited references is “authenticating the client by producing an anonymous signature and opening and maintaining an anonymous authentication session with the server, wherein a unique anonymous signature is used for each session.”

Among the limitations of amended independent claim 15 not present in the cited references is a “system adapted to open and maintain an authentication session guaranteeing non-repudiation, wherein an anonymous signature unique to the session and comprising a series of tokens is used to open and maintain each session, the system comprising ... a first stage in which a client calculates the series of tokens, one of the series of tokens is configured to enable a session to be opened and another of the series of tokens is configured to enable the session to be maintained.”

As discussed above and explicitly recited in the claims, for each session of a user, that user provides the server with a unique anonymous signature. Thus, in the case that two or more

different sessions are started by or otherwise linked to the user, each session cannot have the same anonymous signature, regardless of whether the two or more sessions are still in progress.

Neither Teper nor Camnisch teaches these express recitations of the claims. In Teper, users and Service Providers (“SP”) initially register with an Online Brokering Service (“OBS”). Each user additionally selects a password and is assigned a unique ID, which can be mapped to the user only by the OBS. The password and unique ID are stored in the brokering database, and are used to authenticate registered users during all sessions involving the registered users. (Tepper, col. 2, ln. 57 *et seq.*). This unique ID does not vary with each session opened by any single user.

In Teper, when a user connects to a registered SP site, and attempts to access an online service, the SP site initiates an authentication sequence, which allows the OBS to authenticate the user for the SP site. The SP site sends a challenge message to the user's computer and the user computer responds by generating and returning a cryptographic response message. The cryptographic response message is preferably based on both the challenge message and the user's established password. The SP site forwards the response message to the Online Broker site along with the user's unique ID. (Tepper, col. 3, ln. 5 *et seq.*).

Further, Teper does not teach or suggest an anonymous signature maintaining an anonymous session with a server. The Examiner cited col. 3, lines 5-13 of Teper for this limitation; however, in Teper, the “cryptographic response message” that is returned to the SP by the user's computer is only for opening a session. There is no disclosure in Teper that this response message plays any role in maintaining the session after it is opened.

In Camnisch, a user dealing with an organization has to provide either his real identity or a pseudonym. Specifically, Camnisch relates to a system and method for “securely proving

ownership of pseudonymous or anonymous electronic credentials, wherein a party that proves its ownership of the credential can stay anonymous, i.e., does not need to reveal its identity.” (Camnisch, par. [0006]). Thus, the user’s real identity or pseudonym is not unique for each session.

Neither Teper nor Camnisch teaches or suggests a method wherein a user provides a server or Service Provider (SP) an anonymous signature, which is different for each session. In both Teper and Camnisch, the information provided to the SP or the Organization must remain the same for each session. In fact, nothing in the cited references suggests any limit on the number of sessions using the information or of the validity of the information provided by the user to the SP.

In Feig, a method is disclosed for enforcing the sequential playback of a multimedia file. In one aspect of the disclosed method, a sending server stores a multimedia file which is then partitioned into a plurality of sequential data blocks. The server generates a plurality of enabling tokens, each corresponding to one of the plurality of sequential data blocks. The server then encodes each respective one of the plurality of sequential data blocks with a corresponding one of the plurality of enabling tokens, producing a plurality of encoded sequential data blocks. However, the method in Feig does not disclose “an anonymous signature unique to the session and comprising a series of tokens [that] is used to open and maintain each session, the system comprising ... a first stage in which a client calculates the series of tokens, one of the series of tokens is configured to enable a session to be opened and another of the series of tokens is configured to enable the session to be maintained”, as for example in claim 15.

In contrast, the present claims recite a unique anonymous signature for each session. As described at page 11, lines 4-22 of the present specification, tokens are calculated to enable the

user to open and maintain a session. These tokens correspond to the unique anonymous signature of the claims. Further, the tokens are only for one-time use. (Specification as filed, p. 12, ln. 10; p. 24, ll. 19-26.). As each session for a user is opened, a new unique anonymous signature is produced. The server can then, if required, supply that unique signature to the anonymous certification authority (ACA) and have the user's anonymity revoked. Thus, because Teper, Camnisch and Feig are silent with respect to authenticating the client by producing a unique anonymous signature and opening and maintaining an anonymous authentication session with the server, wherein a unique anonymous signature is used for each session, claims 1 and 15 are deemed to be allowable over the combination of Teper, Camnisch and Feig, whether taken alone or in combination.

Applicants further submit that, beyond the failure of Teper, Camnisch and Feig to teach every limitation of independent claims 1 and 15, there is no teaching or motivation for a person skilled in the art to adapt the teachings of Teper, Camnisch and Feig to arrive at the present invention. In particular, none of the cited references recognize the problem of traceability, as explained at page 5, lines 6-10 of the present application. Specifically, in implementing and using the prior art teachings a server can track the activities of its clients across multiple sessions and thereby develop a detailed profile that includes information of potentially greater benefit than a client's mere real identity. Thus, anonymity is not guaranteed using the prior art teachings, even if combined.

In the case of Teper, a SP dealing with a particular user over a number of different sessions recognizes that user's ID and can easily link the user's different sessions to that particular user. This enables the SP to track the user's activities and to build a customer profile. Indeed, none of the cited references teaches any method or system that keeps information

provided by the user to the SP over a number of different sessions anonymous, so that traceability is not possible.

In contrast, according to the present disclosure and claims, when a user opens up several sessions with the same server, that server will nevertheless be unable to recognize and track the anonymous signatures of that user from session to session since a new and unique anonymous signature is produced for each new session. As a result, the server cannot track the activities, from session to session of a regular but unknown client. This allows for complete anonymity of the user. One skilled in the art would not therefore think to combine Teper, Camnisch and Feig to arrive at the present invention and, thus, the present claims are deemed to be in condition for allowance.

The additional cited references were not added to and do not cure the deficiencies of the references discussed above but, rather, to show additional claim limitations, and do not cure the deficiencies discussed above.

Claims 2-14, 20, and 21 depend from, and contain all of the limitations of, independent claim 1. Claims 16-19 depend from, and contain all of the limitations of, independent claim 15. These dependent claims also recite additional limitations which, in combination with the limitations of the independent claim from which they depend, are neither disclosed nor suggested by the cited references and are also directed to patentable subject matter. Thus, claims 2-14 and 16-21 should also be allowed.

Conclusion

Because the cited prior art references, whether taken alone or in combination, fail to disclose "authenticating the client by producing an anonymous signature and opening and

maintaining an anonymous authentication session with the server, wherein a unique anonymous signature is used for each session," and a system "wherein an anonymous signature unique for each session and comprising a series of tokens is used to open and maintain each session", each of now pending claims 1-21 is deemed to be patentable over that art and in condition for allowance.

A check in the amount \$182.00 is enclosed in payment for the addition of 1 new dependent claim and for a one-month extension of time.

It is believed that no further fees or charges are required at this time in connection with the present application. However, if any additional fees or charges are required at this time, they may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP



By _____
Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: January 12, 2009